AO 106 (Rev. 04/010) Application for Search Warrant AUTHORIZED AND APPROVED/DATE: T. Edgmon 4/30/24

# UNITED STATES DISTRICT COURT

for the

WESTERN DISTRICT OF OKLAHOMA

In the Matter of the Search of )
)
Information associated with Dropbox user )
rickyticky3891@gmail.com )
that is stored at premises controlled by )
Dropbox, Inc. )

Case No: MJ-24-392-STE

## APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

See Attachment A, which is attached and incorporated by reference.

Located in the Northern District of California, there is now concealed:

See Attachment B, which is attached and incorporated by reference.

The basis for the search under Fed. R. Crim.P.41(c) is(*check one or more*):

- ☒ evidence of the crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| 18 U.S.C. § 2252A(a)(5)(B) | Possession of Child Pornography |

The application is based on these facts:

See attached Affidavit of Special Agent Nicholas Ustach, Homeland Security Investigations, which is incorporated by reference herein.

- ☒ Continued on the attached sheet(s).
- ☐ Delayed notice of _____days *(give exact ending date if more than 30 days)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).

*Applicant's signature*

Nicholas Ustach
Special Agent
Homeland Security Investigations

Sworn to before me and signed in my presence.

Date: Apr 30, 2024

*Judge's signature*

City and State: Lawton, OK [redacted]

SHON T. ERWIN, U.S. Magistrate Judge
*Printed name and title*

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF OKLAHOMA

| | |
|---|---|
| IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH DROPBOX USER RICKYTICKY3891@GMAIL.COM THAT IS STORED AT PREMISES CONTROLLED BY DROPBOX, INC. | Case No. MJ-24-392-STE<br>**Filed Under Seal** |

**AFFIDAVIT IN SUPPORT OF**
**AN APPLICATION FOR A SEARCH WARRANT**

I, Nicholas Ustach, being first duly sworn, hereby depose and state as follows:

## INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by Dropbox Inc. ("Dropbox"), an electronic service provider headquartered at 1800 Owens St., Ste. 200 San Francisco, CA 94158. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Dropbox to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

2. I have been employed as a Special Agent ("SA") with Homeland Security Investigations ("HSI") since September 11, 2022. I spent six months at the Federal Law Enforcement Training Center completing the Criminal Investigator Training Program and

HSI Special Agent Training Programs. I previously spent four years employed with US Customs and Border Protection. In the course of my duties, I was exposed to many human and drug smuggling incidents, interviewed parties applying for admission at the Port of Entry, performed searches of vehicles and persons, and processed immigration cases that presented themselves at the port. I participated in multiple discoveries of drugs concealed within vehicles, merchandise, and on persons and performed seizures of the drugs. Before that, I received a Bachelor of Science in Sociology from Brigham Young University and a Master of Science in Criminal Justice from Weber State University.

3. I am currently assigned to HSI Oklahoma City, Oklahoma. As part of my duties, I am tasked with investigating federal criminal cybercrime violations. I have both training and experience conducting child exploitation and child pornography investigations. Moreover, I have access to the institutional knowledge developed around this type of investigation by working with other experienced child exploitation criminal investigators. I have become aware of numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, to include electronic media.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2252A(a)(5)(B)

have been committed by Christopher CARTER using the Dropbox account associated with rickyticky3891@gmail.com. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and fruits of these crimes further described in Attachment B.

## JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

## PROBABLE CAUSE

7. On April 10, 2024, HSI received a National Center for Missing and Exploited Children (NCMEC) CyberTip Report 175784692 for investigation. The CyberTip Report was originally reported to NCMEC by Dropbox Inc. on October 6, 2023, denoting a user uploading twenty-eight (28) files of apparent child pornography. Dropbox provided the files to NCMEC which had been reviewed by a Dropbox representative and were found to be in violation of Dropbox's terms and conditions. The subscriber information provided by Dropbox gave an email of rickyticky3891@gmail.com, a username of Rick Sanchez, and a User ID of 878039475. State search warrants were submitted to both Google and Dropbox for content and information from each account.

8. SA Ustach reviewed an uploaded video named 7c441f3771a6e8c7450091d6a436be05.mp4. The video depicts an adult female performing oral sex on a prepubescent male.

9. SA Ustach reviewed an uploaded video named 0ea37e3d6a57398c98f7b1b4 68a017b.mp4. The video depicts an adult male standing over a prepubescent female that is laying down. The male continually puts his erect penis into the female's mouth.

10. SA Ustach reviewed an uploaded video named 07bfcdd9be4227d58724acd8 69bc9e52.mp4. The video depicts a prepubescent female that is touching and sucking on an erect adult male penis.

11. On March 1, 2024, a response from Google was received in reference to a state search warrant submitted on February 28, 2024, for information associated with rickyticky3891@gmail.com. Located within the Billing Information folder provided by Google, the name Christopher CARTER was found. Located within the Google photos folder were multiple "selfie" photos of a white male. The photos appeared to have been taken from inside a prison cell. There were multiple photos of the male's penis taken from inside the prison cell. One of the photos of the male, shows tattoos on both forearms that read "Pepper Ann" and "Landyn." Similar photos were located in the records received from Dropbox.

12. Law enforcement queries revealed that a male named Christopher B. CARTER, who is Oklahoma Department of Corrections custody in Lawton, OK for Aggravated Possession of Child Pornography and Sexual Abuse of a Child, matches the description of the individual pictured in the photos provided by Google.

13. The first preservation request was submitted to Dropbox on January 31, 2024, prior to the state search warrant. A second preservation request was submitted to Dropbox on April 22, 2024. While Dropbox complied with the prior state search warrant,

more information is needed for the investigation.

## OVERVIEW OF DROPBOX

14. Dropbox is a personal cloud storage service (sometimes referred to as an online backup service) that is frequently used for file sharing and collaboration, which allows users to share files, to include digital images, movies and folders with others across the Internet. Dropbox advertises itself as, "a free service that lets you bring your photos, docs, and videos anywhere and share them easily" (www.dropbox.com).

15. The Dropbox application is available for Windows, Macintosh and Linux desktop operating systems. There are also apps for iPhone, iPad, Android, and BlackBerry devices.

16. To share a file, the user can generate a Uniform Resource Locator (URL) which is a web address for it from the Dropbox website and send it out so that others can view it. Folders can be shared by sending an invitation from the Dropbox website. Recipients that don't have Dropbox accounts will have to sign up to access the folder. Once a folder is shared, it will appear in the folder system for everyone who has access to it and all members will be able to make changes to files. All versions of files are saved.

17. Dropbox provides a variety of on-line services, including online storage access, to the general public. Dropbox allows subscribers to obtain accounts at the domain name www.dropbox.com. Subscribers obtain a Dropbox account by registering with an email address. During the registration process, Dropbox asks subscribers to provide basic personal identifying information. This information can include the subscriber's full name,

physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

18. When the subscriber transfers a file to a Dropbox account, it is initiated at the user's computer, transferred via the Internet to the Dropbox servers, and then can automatically be synchronized and transmitted to other computers or electronic devices that have been registered with that Dropbox account. This includes online storage in Dropbox servers. If the subscriber does not delete the content, the files can remain on Dropbox servers indefinitely. Even if the subscriber deletes their account, it may continue to be available on the Dropbox servers for a certain period of time.

19. Online storage providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, online storage providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

20. In some cases, Dropbox account users will communicate directly with Dropbox about issues relating to the account, such as technical problems, billing inquiries,

or complaints from other users. Online storage providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

21. This application seeks a warrant to search all responsive records and information under the control of Dropbox, a provider subject to the jurisdiction of this court, regardless of where Dropbox has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Dropbox's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

22. As explained herein, information stored in connection with a personal cloud storage service account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with a personal cloud storage service account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, stored communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a

relevant time. Further, information maintained by the provider can show how and when the account was accessed or used. For example, as described below, electronic service providers typically log the Internet Protocol (IP) addresses from which users access the account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the account owner's state of mind as it relates to the offense under investigation. For example, information in the account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

## INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

23. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Dropbox, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of

Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

## CONCLUSION

24. Based on the forgoing, I request that the Court issue the proposed search warrant.

25. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

26. The government will execute this warrant by serving the warrant on Dropbox, Inc. Because the warrant will be served on Dropbox, Inc., who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Nicholas Ustach
Special Agent
Homeland Security Investigations

Sworn and subscribed to before me this 30th day of April 2024.

SHON T. ERWIN
United States Magistrate Judge
Western District of Oklahoma

# ATTACHMENT A

## Property to Be Searched

This warrant applies to information associated with the Dropbox account associated with rickyticky3891@gmail.com that is stored at premises owned, maintained, controlled or operated by Dropbox, Inc. ("Dropbox"), an electronic service provider that accepts service of legal process at 333 Brannan Street, San Francisco, CA 94107.

# ATTACHMENT B

## Particular Things to be Seized

### I. Information to be disclosed by Dropbox (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit card or bank account numbers);

b. The types of service utilized by the user;

c. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

d. All records pertaining to communications between the Provider, and any person regarding the account, including contacts with support services and records of actions taken.

e. All user content created, uploaded, or shared by the account;

f. All content data, including but not limited to file activity logs (i.e., data related to the upload, download, and access of each file); and

g. All images and videos in the account .

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant.

## II. Information to be seized by the government

All information described above in Section I that constitutes evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252A; those violations involving user or users of each account or identifier listed in Attachment A, including information pertaining to the following matters:

a. the production, distribution, receipt or possession of images of child pornography or images of obscene material; or correspondence in furtherance of the

commission of offenses involving the production, distribution, receipt or possession of child pornography or obscene material.

b. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.

c. All images depicting children engaging in sexually explicit conduct as defined in 18 U.S.C. § 2256.